

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования
«Северный (Арктический) федеральный университет имени М.В. Ломоносова»

Высшая школа информационных технологий и автоматизированных систем

ЛАБОРАТОРНАЯ РАБОТА №9

По дисциплине: Защита информации в системах управления базами данных

На тему Защита хоста

Выполнил обучающийся:

Грозов Илья Владимирович

Направление подготовки / специальность:

10.03.01 Информационная безопасность

Курс: 3

Группа: 151113

Руководитель: Зубарев Александр Андреевич, ст.

преподаватель

Отметка о зачете

Руководитель

А.А. Зубарев.

Архангельск 2024

ЗАДАНИЕ

Получить практический навык защиты хоста при эксплуатации СУБД

ХОД РАБОТЫ

1 КОНФИГУРАЦИЯ КОНТЕЙНЕРА DOCKER С DEBAIN

Конфигурация контейнера с debain невозможна в настоящий момент времени. Работа будет выполнена на обычной виртуальной машине Debian 11 с именем ZIvSYBD-LR9

2 ECRYPTFS

2.1 Установка eCryptfs

Выполним установку eCryptfs при помощи команды: `sudo apt-get install eCryptfs-utils`. Выполнение установки eCryptfs отображено на рисунке 1

```
root@ZIVSYBD-LR9:/home/huguenot-lr9# sudo apt-get install eCryptfs-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  keyutils libecryptfs1 libtspil
Suggested packages:
  cryptsetup rsync
The following NEW packages will be installed:
  eCryptfs-utils keyutils libecryptfs1 libtspil
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 366 kB of archives.
After this operation, 1,335 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Рисунок 1 – Выполнение установки eCryptfs

Завершение установки eCryptfs отображено на рисунке 2

```
Get:1 http://deb.debian.org/debian bullseye/main amd64 libecryptfs1 amd64 1:1.1-5 [42.8 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 libtspil amd64 0.3.14+fixed1-1.2 [168 kB]
Get:3 http://deb.debian.org/debian bullseye/main amd64 keyutils amd64 1.6.1-2 [52.8 kB]
Get:4 http://deb.debian.org/debian bullseye/main amd64 eCryptfs-utils amd64 1:1.1-5 [102 kB]
Fetched 366 kB in 0s (744 kB/s)
Selecting previously unselected package libecryptfs1.
(Reading database ... 165440 files and directories currently installed.)
Preparing to unpack .../libecryptfs1_1:1.1-5_amd64.deb ...
Unpacking libecryptfs1 (1:1.1-5) ...
Selecting previously unselected package libtspil.
Preparing to unpack .../libtspil_0.3.14+fixed1-1.2_amd64.deb ...
Unpacking libtspil (0.3.14+fixed1-1.2) ...
Selecting previously unselected package keyutils.
Preparing to unpack .../keyutils_1.6.1-2_amd64.deb ...
Unpacking keyutils (1.6.1-2) ...
Selecting previously unselected package eCryptfs-utils.
Preparing to unpack .../eCryptfs-utils_1:1.1-5_amd64.deb ...
Unpacking eCryptfs-utils (1:1.1-5) ...
Setting up libtspil (0.3.14+fixed1-1.2) ...
Setting up libecryptfs1 (1:1.1-5) ...
Setting up keyutils (1.6.1-2) ...
Setting up eCryptfs-utils (1:1.1-5) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for libc-bin (2.31-13+deb11u10) ...
root@ZIVSYBD-LR9:/home/huguenot-lr9#
```

Рисунок 2 – Завершение установки eCryptfs

2.2 Добавление пользователя cryptouser

Добавим пользователя cryptouser при помощи команды: `sudo adduser cryptouser`. Добавление пользователя cryptouser отображено на рисунке 3

```
root@ZIVSYBD-LR9:/home/huguenot-lr9# sudo adduser cryptouser
Adding user `cryptouser' ...
Adding new group `cryptouser' (1001) ...
Adding new user `cryptouser' (1001) with group `cryptouser' ...
Creating home directory `/home/cryptouser' ...
Copying files from `/etc/skel' ...
New password: █
```

Рисунок 3 – Добавление пользователя cryptouser

Установим для пользователя cryptouser пароль и запрашиваемые данные. Установка пароля и запрашиваемых данных для пользователя cryptouser отображена на рисунке 4

```
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for cryptouser
Enter the new value, or press ENTER for the default
  Full Name []: cryptouser
  Room Number []: cryptouser
  Work Phone []: cryptouser
  Home Phone []: cryptouser
  Other []: cryptouser
Is the information correct? [Y/n] Y
root@ZIVSYBD-LR9:/home/huguenot-lr9# █
```

Рисунок 4 – Установка пароля для пользователя cryptouser и запрашиваемых данных

Сменим пользователя на cryptouser для проверки корректности его создания. Смена пользователя отображена на рисунке 5

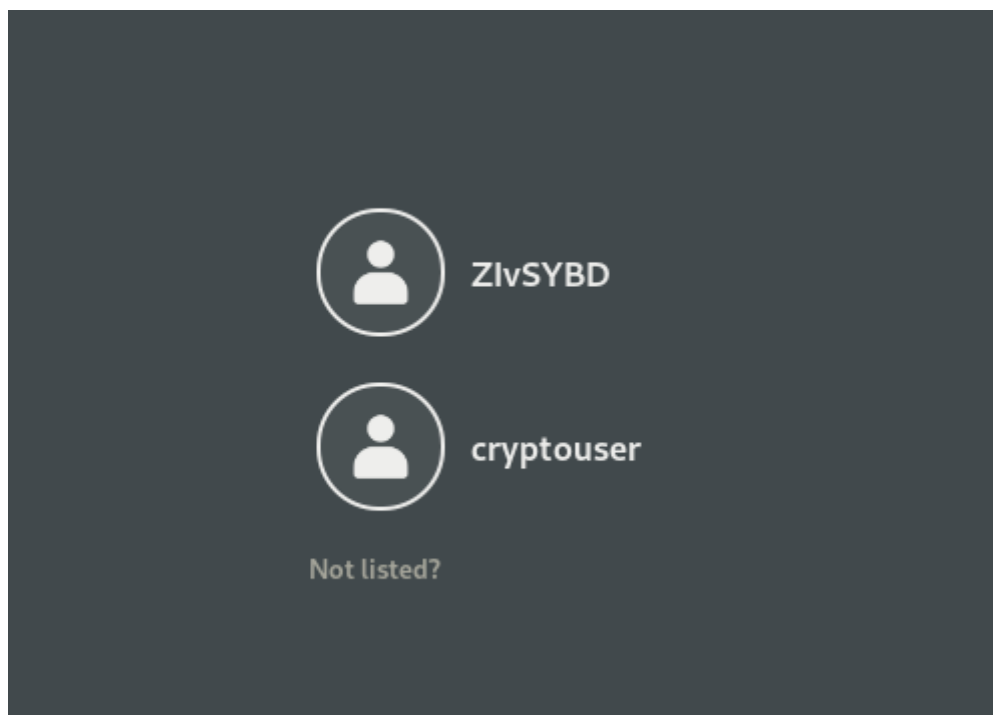


Рисунок 5 – смена пользователя

Рабочий пользователь cryptouser отображен на рисунке 6

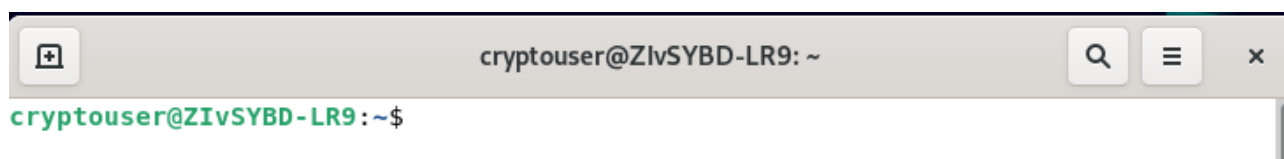


Рисунок 6 – Рабочий пользователь cryptouser

2.3 Шифрование домашнего каталога пользователя с помощью eCryptfs

Выполним шифрование домашней директории пользователя cryptouser. Перед выполнением шифрования нам необходимо дополнительно установить rsync. Установка rsync отображена на рисунке 7

```

root@ZIVSYBD-LR9:/home/huguenot-lr9# sudo apt-get install rsync
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  openssh-server
The following NEW packages will be installed:
  rsync
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 396 kB of archives.
After this operation, 755 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 rsync amd64 3.2.3-4+deb11u1 [396 kB]
Fetched 396 kB in 0s (936 kB/s)
Selecting previously unselected package rsync.
(Reading database ... 165538 files and directories currently installed.)
Preparing to unpack .../rsync 3.2.3-4+deb11u1_amd64.deb ...
Unpacking rsync (3.2.3-4+deb11u1) ...
Setting up rsync (3.2.3-4+deb11u1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/rsync.service → /lib/systemd/system/rsync.service.
Processing triggers for man-db (2.9.4-2) ...
root@ZIVSYBD-LR9:/home/huguenot-lr9#

```

Рисунок 7 – Установка rsync

Выполним шифрование домашнего каталога пользователя cryptouser при помощи команды `sudo-ecryptfs-migrate-home -u cryptouser`. Шифрование домашнего каталога пользователя cryptouser отображено на рисунке 8

```

root@ZIVSYBD-LR9:/home/huguenot-lr9# sudo ecryptfs-migrate-home -u cryptouser
INFO: Checking disk space, this may take a few moments. Please be patient.
INFO: Checking for open files in /home/cryptouser
lsuf: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
Output information may be incomplete.
lsuf: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.
INFO: The following files are in use:

lsuf: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
Output information may be incomplete.
lsuf: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.

```

Рисунок 8 – Шифрование домашнего каталога пользователя cryptouser

Шифрование было завершено неудачно. Было выяснено, что его невозможно произвести, поскольку системными процессами были открыты файлы, которые не позволяют завершить процесс шифрования. Создадим пользователя cryptouser2 для шифрования его домашнего каталога. Создание пользователя cryptouser2 отображено на рисунке 9

```
root@ZIVSYBD-LR9:/home/huguenot-lr9# sudo adduser cryptouser2
Adding user `cryptouser2' ...
Adding new group `cryptouser2' (1002) ...
Adding new user `cryptouser2' (1002) with group `cryptouser2' ...
Creating home directory `/home/cryptouser2' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for cryptouser2
Enter the new value, or press ENTER for the default
    Full Name []: cryptouser2
    Room Number []: cryptouser2
    Work Phone []: cryptouser2
    Home Phone []: cryptouser2
    Other []: cryptouser2
Is the information correct? [Y/n] Y
```

Рисунок 9 – Создание пользователя cryptouser2

Выполним шифрование домашнего каталога пользователя cryptouser2 при помощи команды: `sudo-ecryptfs-migrate-home -u cryptouser2`. Выполнение шифрования отображено на рисунке 10

```
root@ZIVSYBD-LR9:/home/huguenot-lr9# sudo ecryptfs-migrate-home -u cryptouser2
INFO: Checking disk space, this may take a few moments. Please be patient.
INFO: Checking for open files in /home/cryptouser2
lsuf: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
Output information may be incomplete.
lsuf: WARNING: can't stat() fuse.portal file system /run/user/1000/doc
Output information may be incomplete.
ERROR: Cannot get ecryptfs version, ecryptfs kernel module not loaded?
```

Рисунок 10 – Выполнение шифрования

Шифрование домашнего каталога пользователя cryptouser2 не было произведено из-за того, что не был загружен модуль. Загрузим модуль при помощи команды: `sudo modprobe ecryptfs`. Загрузка модуля отображена на рисунке 11

```
root@ZIVSYBD-LR9:/home/huguenot-lr9# sudo modprobe ecryptfs
```

Рисунок 11 – Загрузка модуля

Модуль загружен. Выполним шифрование домашнего каталога пользователя cryptouser2 при помощи команды: `sudo-ecryptfs-migrate-home -u cryptouser2`. Выполнение шифрования отображено на рисунке 12


```

root@ZiVSYBD-LR9:/home/huguenot-lr9# sudo ecryptfs-migrate-home -u cryptouser2
INFO: Checking disk space, this may take a few moments. Please be patient.
INFO: Checking for open files in /home/cryptouser2
lsuf: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
Output information may be incomplete.
lsuf: WARNING: can't stat() fuse.portal file system /run/user/1000/doc
Output information may be incomplete.
Enter your login passphrase [cryptouser2]:

```

Рисунок 12 – Выполнение шифрования

Введем установленный пароль. После ввода пароля необходимо воспользоваться информацией выведенной в заметке. Заметка отображена на рисунке 13

```

*****
YOU SHOULD RECORD YOUR MOUNT PASSPHRASE AND STORE IT IN A SAFE LOCATION.
ecryptfs-unwrap-passphrase ~/.ecryptfs/wrapped-passphrase
THIS WILL BE REQUIRED IF YOU NEED TO RECOVER YOUR DATA AT A LATER TIME.
*****

Done configuring.

chown: cannot access '/dev/shm/.ecryptfs-cryptouser2': No such file or directory
INFO: Encrypted home has been set up, encrypting files now...this may take a while.
sending incremental file list
./
.bash_logout      220 100%    0.00kB/s    0:00:00 (xfr#1, to-chk=2/4)
.bashrc           3,526 100%    3.36MB/s    0:00:00 (xfr#2, to-chk=1/4)
.profile          807 100%   788.09kB/s    0:00:00 (xfr#3, to-chk=0/4)
Could not unlink the key(s) from your keyring. Please use `keyctl unlink` if you wish to remove the key(s). Proceeding with umount.

=====
Some Important Notes!

1. The file encryption appears to have completed successfully, however,
   cryptouser2 MUST LOGIN IMMEDIATELY, _BEFORE THE NEXT REBOOT_,
   TO COMPLETE THE MIGRATION!!!

2. If cryptouser2 can log in and read and write their files, then the migration is complete,
   and you should remove /home/cryptouser2.GNq5LAoP.
   Otherwise, restore /home/cryptouser2.GNq5LAoP back to /home/cryptouser2.

3. cryptouser2 should also run 'ecryptfs-unwrap-passphrase' and record
   their randomly generated mount passphrase as soon as possible.

4. To ensure the integrity of all encrypted data on this system, you
   should also encrypt swap space with 'ecryptfs-setup-swap'.
=====

root@ZiVSYBD-LR9:/home/huguenot-lr9#

```

Рисунок 13 – Заметка

Авторизуемся под пользователем cryptouser2. Авторизация под пользователем cryptouser2. Авторизация под пользователем cryptouser2 отображена на рисунке 14

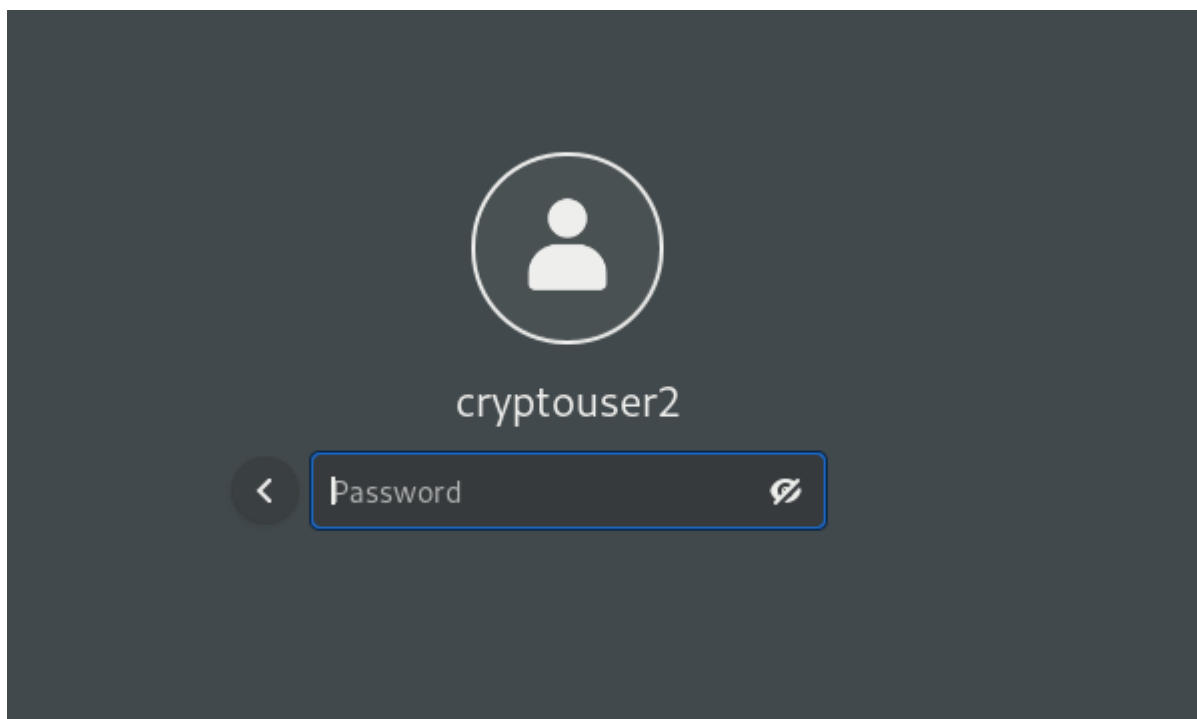


Рисунок 14 – Авторизация под пользователем cryptouser2

По информации в заметке удалим каталог cryptouser2.Gna5LAoP при помощи команды `sudo rm -r cryptouser2.Gna5LAoP`. Удаление каталога cryptouser2.Gna5LAoP отображено на рисунке 15

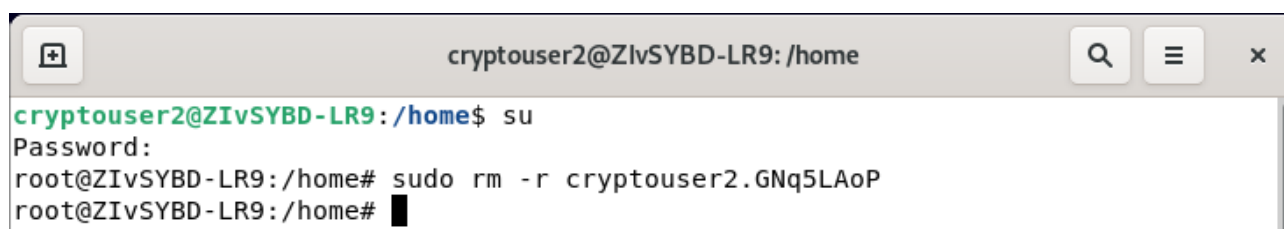


Рисунок 15 – Удаление каталога cryptouser2.Gna5LAoP

При помощи команды `ecryptfs-unwrap-passphrase` узнаем пароль для восстановления зашифрованного раздела. Получение пароля для восстановления отображено на рисунке 16

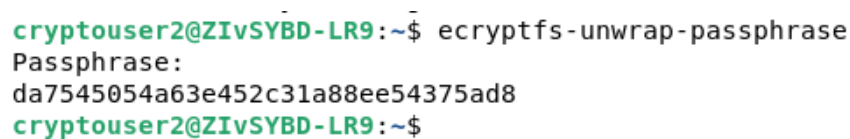
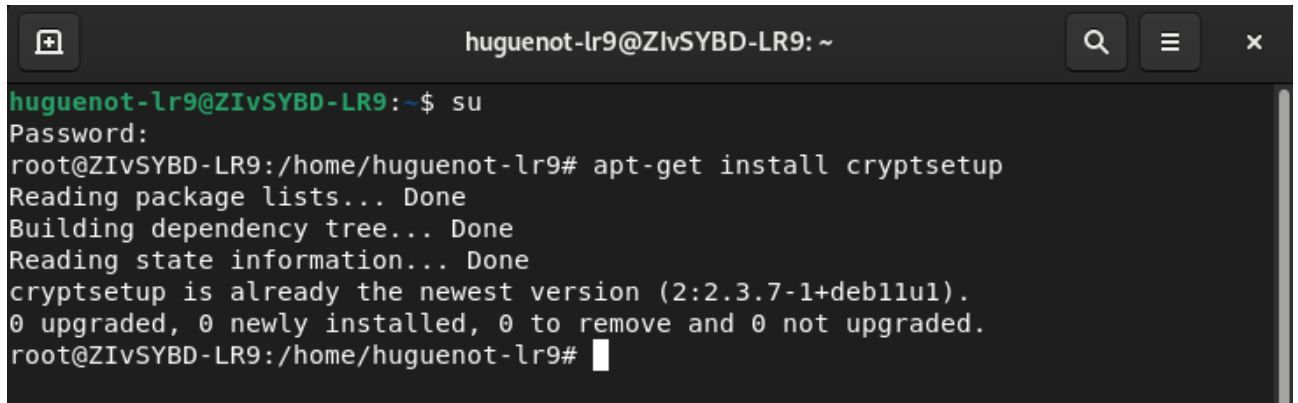


Рисунок 16 – Получение пароля для восстановления

3 LUKS

3.1 Установка поддержки luks

Установим luks при помощи команды: `apt-get install cryptsetup`.
Установленный cryptsetup отображен на рисунке 17

A screenshot of a terminal window with a dark background. The window title is 'huguenot-lr9@ZlvSYBD-LR9: ~'. The terminal shows a user switching to root with 'su', entering a password, and then running 'apt-get install cryptsetup'. The output indicates that cryptsetup is already installed at the latest version (2:2.3.7-1+deb11u1) and no action is needed. The prompt returns to root@ZlvSYBD-LR9: /home/huguenot-lr9#.

```
huguenot-lr9@ZlvSYBD-LR9:~$ su
Password:
root@ZlvSYBD-LR9:/home/huguenot-lr9# apt-get install cryptsetup
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
cryptsetup is already the newest version (2:2.3.7-1+deb11u1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@ZlvSYBD-LR9:/home/huguenot-lr9#
```

Рисунок 17 – Установленный cryptsetup

3.2 Создание раздела

Для создания нового раздела под шифрование с luks воспользуемся инструментами virtualbox за место утилит Debian и создадим диск. В настройках виртуальной машины добавим новый диск. Добавление нового диска отображено на рисунке 18

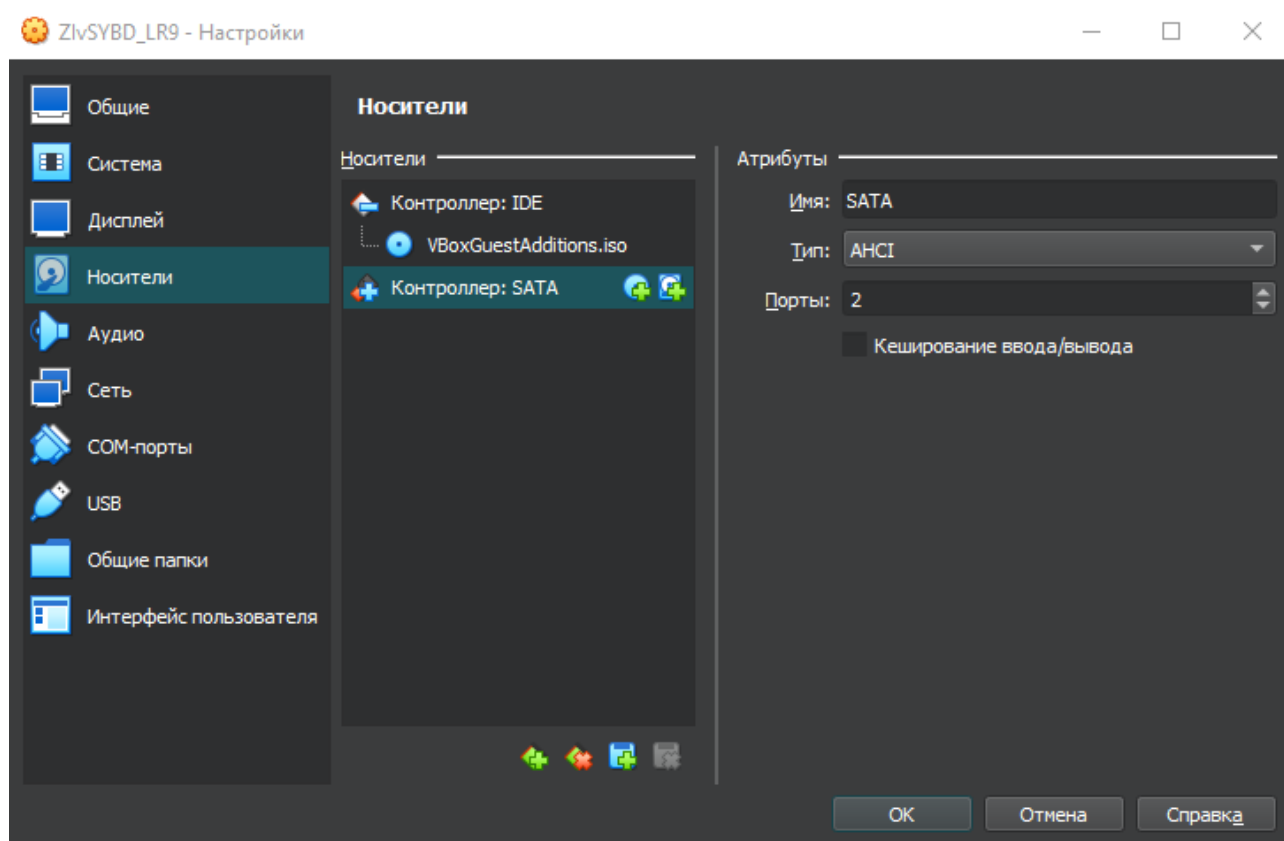


Рисунок 18 – Добавление нового диска

Создадим новый диск с предложенным размером в 100 мегабайт. Создание диска отображено на рисунке 19

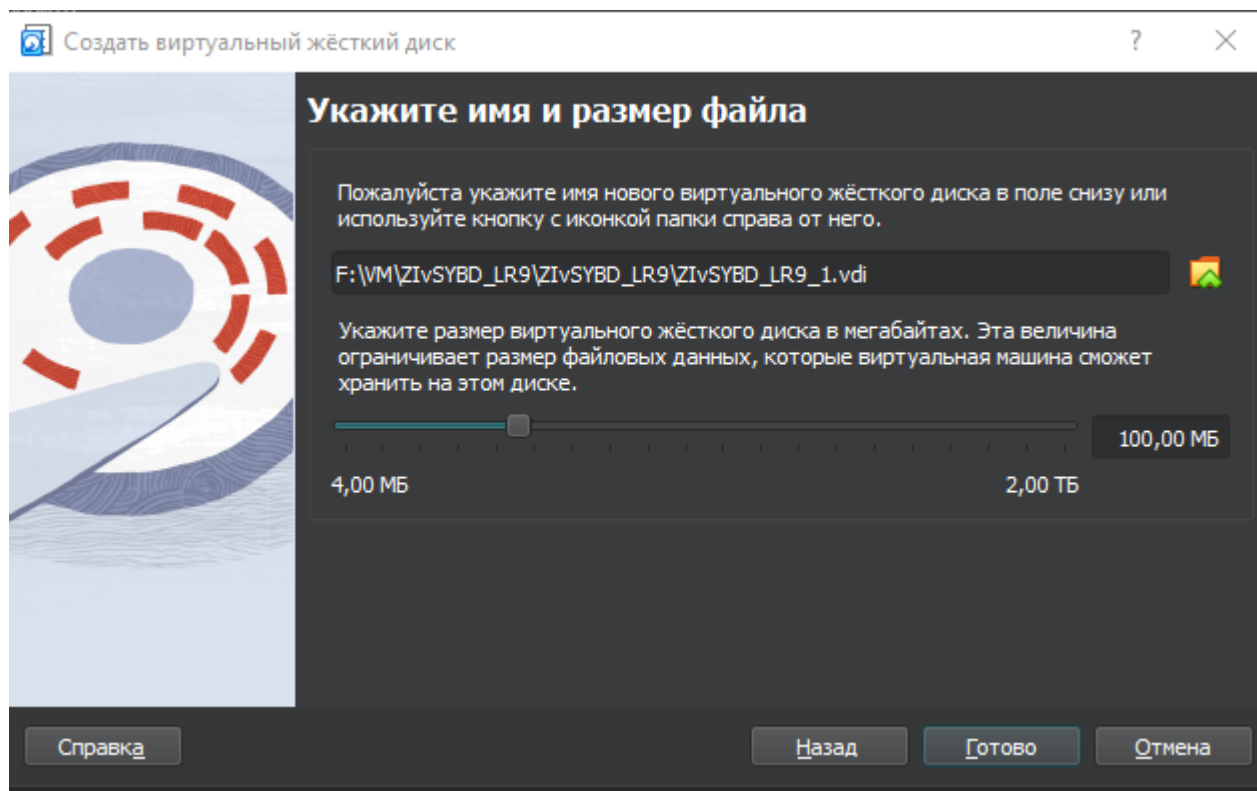


Рисунок 19 – Создание нового диска

Созданный новый диск отображен на рисунке 20

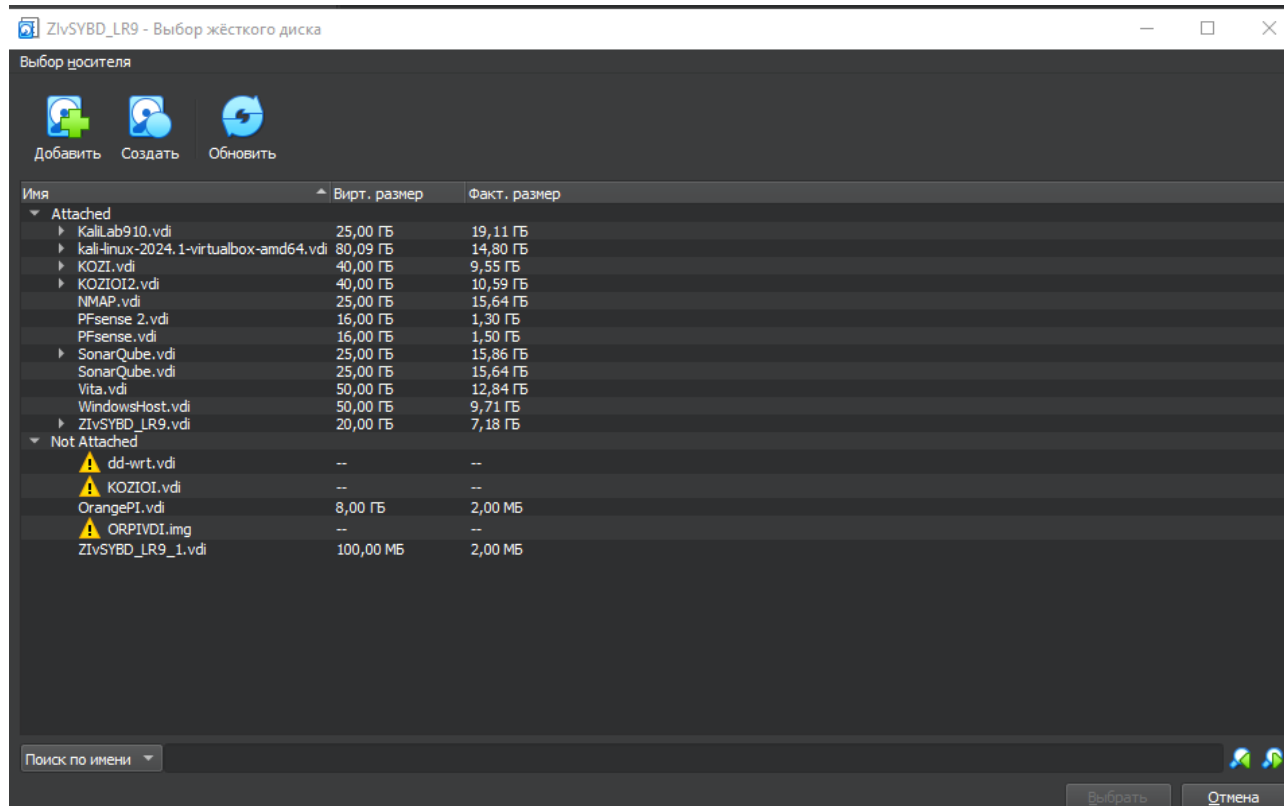


Рисунок 20 – Созданный новый диск

Подключим диск к виртуальной машине. Подключенный диск к виртуальной машине отображен на рисунке 21

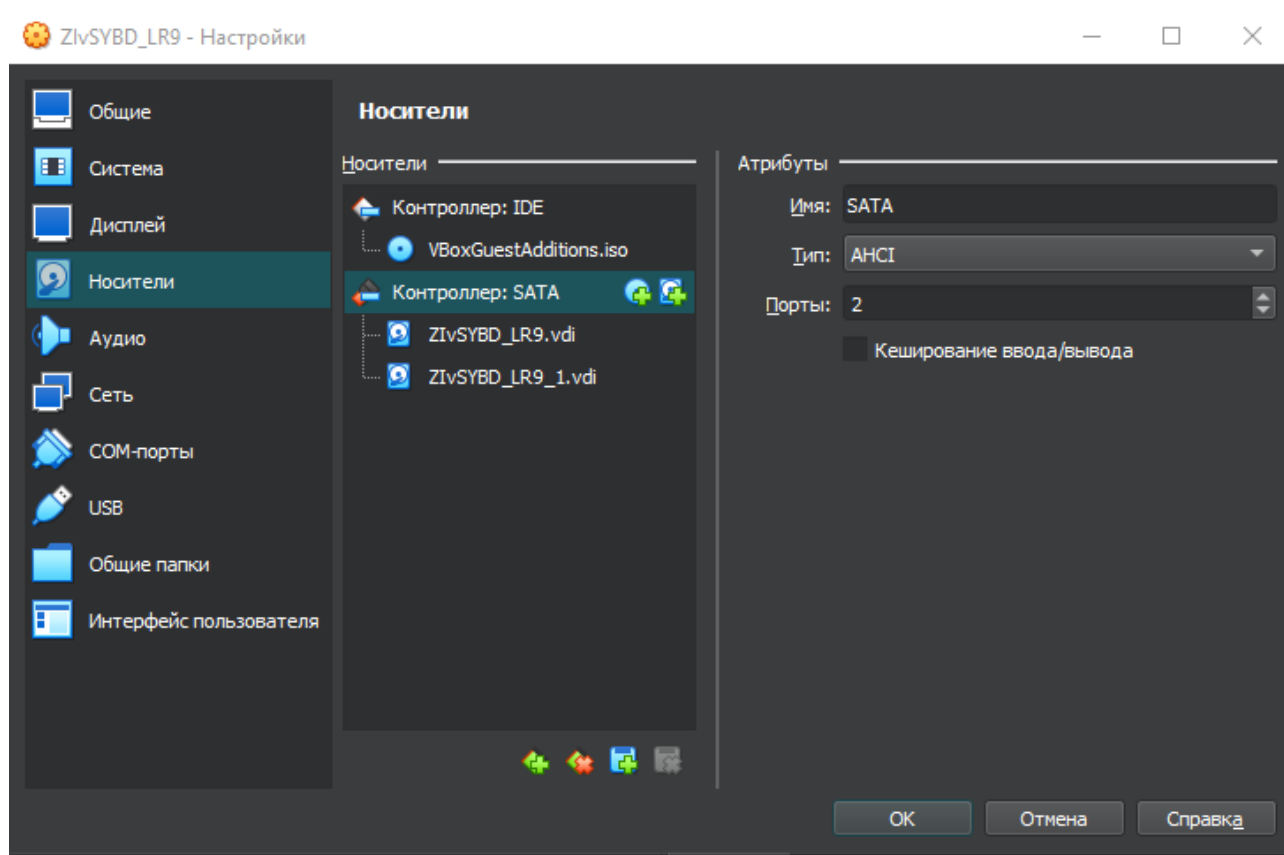


Рисунок 21 – Подключенный диск к виртуальной машине

При помощи команды `lsblk` посмотрим, что диск виден системой. Просмотр диска отображен на рисунке 22

```
root@ZivSYBD-LR9:/home/huguenot-lr9# lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda          8:0    0   20G  0 disk
├─sda1       8:1    0   19G  0 part /
├─sda2       8:2    0    1K  0 part
└─sda5       8:5    0   975M  0 part [SWAP]
sdb          8:16    0   100M  0 disk
sr0         11:0    1   50.5M  0 rom
root@ZivSYBD-LR9:/home/huguenot-lr9#
```

Рисунок 22 – Просмотр диска

Новый диск был зарегистрирован в системе под именем `sdb`

3.3 Шифрование созданного раздела

Выполним шифрование при помощи команды: `sudo cryptsetup luksFormat /dev/sdb`. Подтвердим свои действия введя заглавными буквами YES. Введем пароль по требованию. Завершенное шифрование отображено на рисунке 23

```
root@ZiVSYBD-LR9:/home/huguenot-lr9# sudo cryptsetup luksFormat /dev/sdb

WARNING!
=====
This will overwrite data on /dev/sdb irrevocably.

Are you sure? (Type 'yes' in capital letters): YES
Enter passphrase for /dev/sdb:
Verify passphrase:

root@ZiVSYBD-LR9:/home/huguenot-lr9#
root@ZiVSYBD-LR9:/home/huguenot-lr9#
root@ZiVSYBD-LR9:/home/huguenot-lr9#
```

Рисунок 23 – Завершенное шифрование

4 APPARMOR

4.1 Установка apparmor

Выполним установку при помощи `apt-get install apparmor`. Установка apparmor отображена на рисунке 24

```
root@ZiVSYBD-LR9:/home/huguenot-lr9# apt-get install apparmor
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apparmor is already the newest version (2.13.6-10).
apparmor set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@ZiVSYBD-LR9:/home/huguenot-lr9#
```

Рисунок 24 – Установка apparmor

Установим дополнительный пакет утилит при помощи команды: `apt-get install apparmor-utils`. Установка дополнительного пакета отображена на рисунке 25

```
root@ZiVSYBD-LR9:/home/huguenot-lr9# apt-get install apparmor-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-apparmor python3-libapparmor
Suggested packages:
  vim-addon-manager
The following NEW packages will be installed:
  apparmor-utils python3-apparmor python3-libapparmor
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 383 kB of archives.
After this operation, 1,137 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://deb.debian.org/debian bullseye/main amd64 python3-libapparmor amd64 2.13.6-10 [94.6 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 python3-apparmor amd64 2.13.6-10 [146 kB]
Get:3 http://deb.debian.org/debian bullseye/main amd64 apparmor-utils amd64 2.13.6-10 [142 kB]
Fetched 383 kB in 0s (832 kB/s)
Selecting previously unselected package python3-libapparmor.
(Reading database ... 165739 files and directories currently installed.)
Preparing to unpack .../python3-libapparmor_2.13.6-10_amd64.deb ...
Unpacking python3-libapparmor (2.13.6-10) ...
```

Рисунок 25 – Установка дополнительного пакета

При помощи команды: `systemctl status apparmor` проверим, что apparmor запущен в системе. Проверка запуска apparmor в системе отображена на рисунке 26


```

root@ZiVSYBD-LR9:/home/huguenot-lr9# systemctl status apparmor
● apparmor.service - Load AppArmor profiles
   Loaded: loaded (/lib/systemd/system/apparmor.service; enabled; vendor preset: enabled)
   Active: active (exited) since Sat 2024-06-01 15:30:24 MSK; 20min ago
     Docs: man:apparmor(7)
           https://gitlab.com/apparmor/apparmor/wikis/home/
   Process: 320 ExecStart=/lib/apparmor/apparmor.systemd reload (code=exited, status=0/SUCCESS)
  Main PID: 320 (code=exited, status=0/SUCCESS)
    CPU: 250ms

Jun 01 15:30:24 ZiVSYBD-LR9 apparmor.systemd[320]: Restarting AppArmor
Jun 01 15:30:24 ZiVSYBD-LR9 apparmor.systemd[320]: Reloading AppArmor profiles
Jun 01 15:30:23 ZiVSYBD-LR9 systemd[1]: Starting Load AppArmor profiles...
Jun 01 15:30:24 ZiVSYBD-LR9 systemd[1]: Finished Load AppArmor profiles.
root@ZiVSYBD-LR9:/home/huguenot-lr9#

```

Рисунок 26 – Проверка запуска apparmor в системе

Дополнительно загрузим пакет с профилями при помощи команды `apparmor-profiles`. Загрузка пакета с профилями отображена на рисунке 27

```

root@ZiVSYBD-LR9:/home/huguenot-lr9# sudo apt-get install apparmor-profiles
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  apparmor-profiles
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 99.1 kB of archives.
After this operation, 356 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 apparmor-profiles all 2.13.6-10 [99.1 kB]
Fetched 99.1 kB in 0s (334 kB/s)
Selecting previously unselected package apparmor-profiles.
(Reading database ... 165831 files and directories currently installed.)
Preparing to unpack .../apparmor-profiles_2.13.6-10_all.deb ...
Unpacking apparmor-profiles (2.13.6-10) ...
Setting up apparmor-profiles (2.13.6-10) ...
root@ZiVSYBD-LR9:/home/huguenot-lr9#

```

Рисунок 27 – Загрузка пакета с профилями

Проверим статус работы apparmor при помощи команды: `sudo apparmor_status`. Проверка статуса работы apparmor отображена на рисунке 28

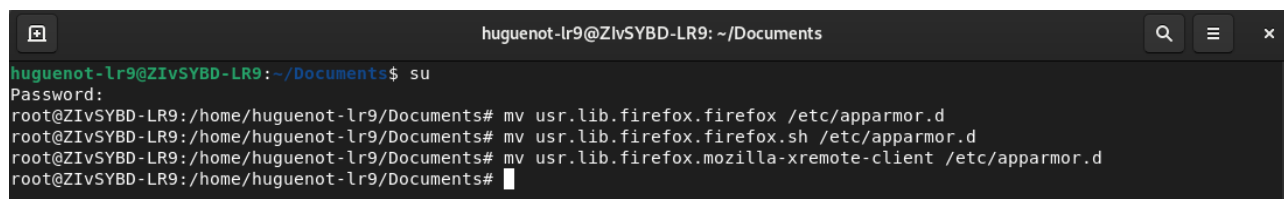
```

Preparing to unpack .../apparmor-profiles_2.13.6-10_all.deb ...
Unpacking apparmor-profiles (2.13.6-10) ...
Setting up apparmor-profiles (2.13.6-10) ...
root@ZIVSYBD-LR9:/home/huguenot-lr9# sudo apparmor_status
apparmor module is loaded.
35 profiles are loaded.
18 profiles are in enforce mode.
  /usr/bin/evince
  /usr/bin/evince-previewer
  /usr/bin/evince-previewer//sanitized_helper
  /usr/bin/evince-thumbnailer
  /usr/bin/evince//sanitized_helper
  /usr/bin/man
  /usr/lib/cups/backend/cups-pdf
  /usr/sbin/cups-browsed
  /usr/sbin/cupsd
  /usr/sbin/cupsd//third_party
  libreoffice-senddoc
  libreoffice-soffice//gpg
  libreoffice-xpdfimport
  lsb_release
  man_filter
  man_groff
  nvidia_modprobe
  nvidia_modprobe//kmod
17 profiles are in complain mode.
  /usr/sbin/dnsmasq
  /usr/sbin/dnsmasq//libvirt_leaseshelper
  avahi-daemon
  identd
  klogd
  libreoffice-oopslash
  libreoffice-soffice
  mDNSd
  nmbd
  nscd
  ping
  smbd
  smbldap-useradd
  smbldap-useradd///etc/init.d/nscd
  syslog-ng
  syslogd
  traceroute
2 processes have profiles defined.
2 processes are in enforce mode.
  /usr/sbin/cups-browsed (592)
  /usr/sbin/cupsd (544)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
root@ZIVSYBD-LR9:/home/huguenot-lr9#

```

Рисунок 28 – Проверка статуса работы apparmor

При необходимости выполним перемещение ранее загруженных необходимых профилей при помощи команды mv. Перемещение профилей отображено на рисунке 29

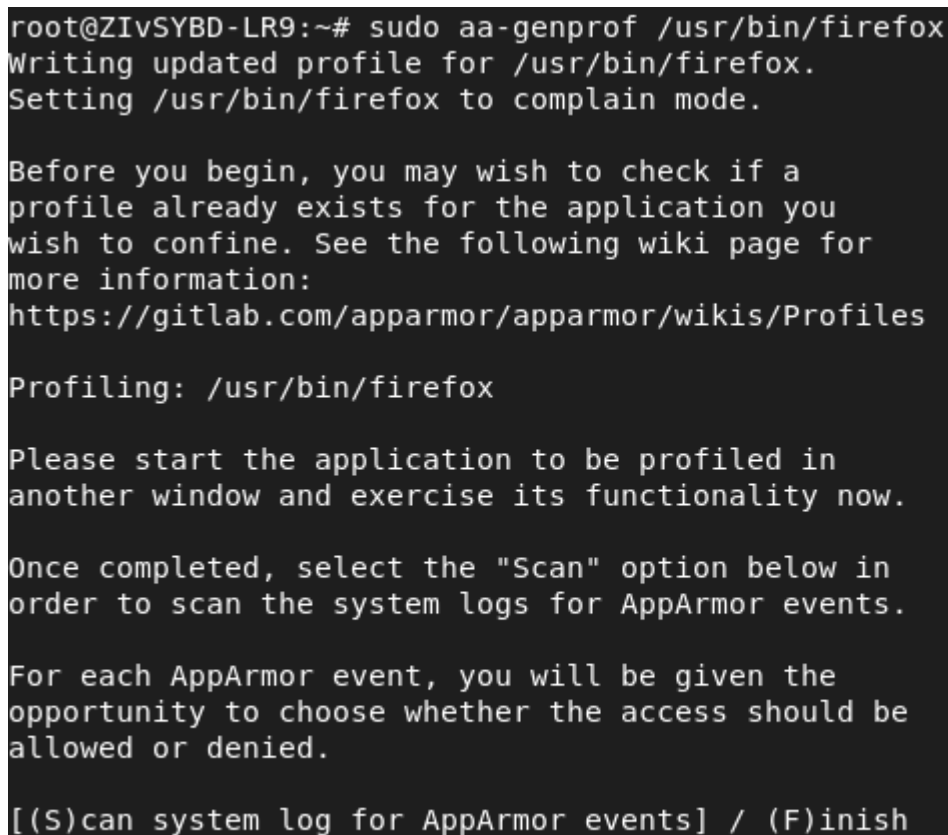


```
huguenot-lr9@ZivSYBD-LR9: ~/Documents
huguenot-lr9@ZivSYBD-LR9:~/Documents$ su
Password:
root@ZivSYBD-LR9:/home/huguenot-lr9/Documents# mv usr.lib.firefox.firefox /etc/apparmor.d
root@ZivSYBD-LR9:/home/huguenot-lr9/Documents# mv usr.lib.firefox.firefox.sh /etc/apparmor.d
root@ZivSYBD-LR9:/home/huguenot-lr9/Documents# mv usr.lib.firefox.mozilla-xremote-client /etc/apparmor.d
root@ZivSYBD-LR9:/home/huguenot-lr9/Documents#
```

Рисунок 29 – Перемещение профилей

4.2 Выполнение блокирования и разблокирования приложения

При помощи команды `sudo aa-genprof /usr/bin/firefox` начнем запись для последующей блокировки приложения. Путь указывает на расположение бинарного файла блокируемого приложения. В качестве блокируемого приложения был выбран браузер `firefox`. Запись для блокировки приложения отображена на рисунке 30



```
root@ZIVSYBD-LR9:~# sudo aa-genprof /usr/bin/firefox
Writing updated profile for /usr/bin/firefox.
Setting /usr/bin/firefox to complain mode.

Before you begin, you may wish to check if a
profile already exists for the application you
wish to confine. See the following wiki page for
more information:
https://gitlab.com/apparmor/apparmor/wikis/Profiles

Profiling: /usr/bin/firefox

Please start the application to be profiled in
another window and exercise its functionality now.

Once completed, select the "Scan" option below in
order to scan the system logs for AppArmor events.

For each AppArmor event, you will be given the
opportunity to choose whether the access should be
allowed or denied.

[(S)can system log for AppArmor events] / (F)inish
```

Рисунок 30 – Запись для блокирования приложения

Войдем в браузер, сделаем хаотичные действия, введем запрос кто такие гугеноты. Хаотичные действия в браузере отображены на рисунке 31

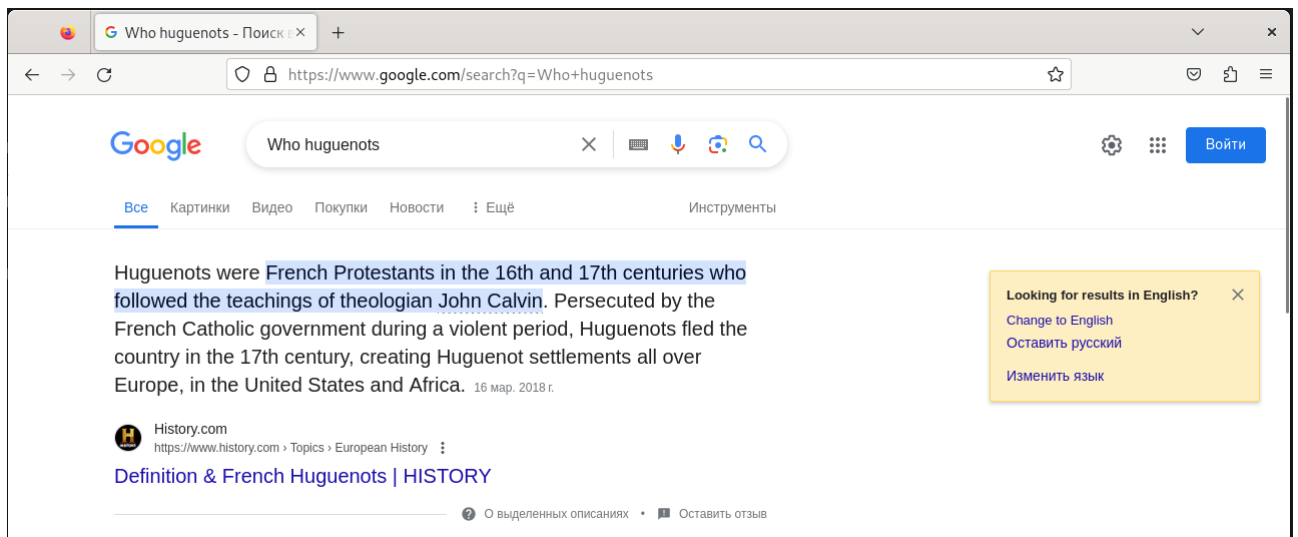


Рисунок 31 – Хаотичные действия в браузере

Для простора событий можно использовать клавишу S, Просмотр событий отображен на рисунке 32

```
Once completed, select the "Scan" option below in
order to scan the system logs for AppArmor events.

For each AppArmor event, you will be given the
opportunity to choose whether the access should be
allowed or denied.
```

Рисунок 32 – Просмотр событий

Остановить запись для блокирования приложения можно по клавише F. Остановка записи отображена на рисунке 33

```
[(S)can system log for AppArmor events] / (F)inish
Setting /usr/bin/firefox to enforce mode.

Reloaded AppArmor profiles in enforce mode.

Please consider contributing your new profile!
See the following wiki page for more information:
https://gitlab.com/apparmor/apparmor/wikis/Profiles

Finished generating profile for /usr/bin/firefox.
root@ZiVSYBD-LR9:~#
```

Рисунок 33 – Остановка записи событий

Теперь приложение должно быть заблокировано. Попробуем запустить приложение из терминала. Попытка запуска приложения отображена на рисунке 43

```
root@ZiVSYBD-LR9:~# firefox
/usr/bin/firefox: 6: exec: firefox-esr: Permission denied
root@ZiVSYBD-LR9:~#
```

Рисунок 34 – Попытка запуска приложения

Приложение заблокировано

4.3 Удаление apparmor

Перед удалением apparmor необходимо остановить его системный процесс при помощи команды: `/etc/init.d/apparmor stop`. Остановка системного процесса apparmor отображена на рисунке 35

```
root@ZiVSYBD-LR9:~# /etc/init.d/apparmor stop
Stopping apparmor (via systemctl): apparmor.service.
root@ZiVSYBD-LR9:~#
```

Рисунок 35 – Остановка системного процесса apparmor

Выполним удаление apparmor и его зависимостей при помощи команды: `sudo apt-get remove apparmor -y`. Удаление apparmor и его зависимостей отображено на рисунке 36

```
root@ZiVSYBD-LR9:~# sudo apt-get remove apparmor -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  python3-apparmor python3-libapparmor
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  apparmor apparmor-profiles apparmor-utils
0 upgraded, 0 newly installed, 3 to remove and 0 not upgraded.
After this operation, 3,368 kB disk space will be freed.
(Reading database ... 165972 files and directories currently installed.)
Removing apparmor-profiles (2.13.6-10) ...
Removing apparmor-utils (2.13.6-10) ...
Removing apparmor (2.13.6-10) ...
Processing triggers for man-db (2.9.4-2) ...
root@ZiVSYBD-LR9:~#
```

Рисунок 36 – Удаление apparmor и его зависимостей

Завершающим действием можно удалить пустые папки при помощи команды: `rm -rf /etc/apparmor /etc/apparmor.d`. Удаление пустых папок отображено на рисунке 37



```
root@ZIvSYBD-LR9:~# rm -rf /etc/apparmor /etc/apparmor.d
root@ZIvSYBD-LR9:~#
```

Рисунок 37 – Удаление пустых папок

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое eCryptfs? Где применяет? Какие алгоритмы шифрования поддерживает?

eCryptfs (Enterprise Cryptographic File System) — это программа для шифрования файловой системы, которая предназначена для защиты данных. eCryptfs широко используется в Linux-системах для шифрования конфиденциальных данных на диске, например, в домашних каталогах пользователей или в облачных хранилищах. Алгоритмы шифрования, поддерживаемые eCryptfs, включают в себя AES

2. Что такое LUKS? Где применяет? Какие алгоритмы шифрования поддерживает?

LUKS (Linux Unified Key Setup) — это стандарт для шифрования дисков в операционных системах Linux. Он предоставляет прозрачное шифрование целых блочных устройств, таких как жесткие диски или разделы диска. LUKS используется для шифрования данных на уровне блочных устройств и обеспечивает высокий уровень безопасности. Он часто применяется для защиты конфиденциальных данных на ноутбуках, серверах или других устройствах. LUKS поддерживает различные алгоритмы шифрования, включая: AES, Twofish

3. Что такое apparmor ? Какие правила могут быть использованны? С какими объектами работает apparmor?

AppArmor (Application Armor) — это система безопасности для контроля доступа к файлам, директориям и другим ресурсам на уровне приложений в операционных системах Linux. Она позволяет определить правила доступа для конкретных приложений, ограничивая их возможности доступа к определенным ресурсам. Правила в AppArmor могут быть использованы для

определения, какие файлы, директории и другие ресурсы могут быть доступны приложению. `ppArmor` работает с различными объектами, такими как исполняемые файлы приложений, библиотеки, конфигурационные файлы и другие ресурсы, к которым приложение может обращаться во время своей работы

ВЫВОД

В ходе выполнения лабораторной работы по теме: «Защита хоста» получили практический навык защиты хоста при эксплуатации СУБД